CUSTOMER NO.: 24498
Serial No.: 09/445,132
Final Office Action dated: October 3, 2005
Response dated: December 7, 2005

PATENT
RCA 88,637

Listing and Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims 1-6 (Cancelled)

7. (Currently amended) The method of Claim ~~22~~ 21 wherein said digital certificate, said ~~first~~ public key and said first private key are issued by an independent certificate authority and are associated with said second device.

8. (Previously Presented) The method of Claim 7 wherein said first device is a set-top box and said second device is a server associated with a service provider, the set-top box having a smart card with service provider identification data stored therein coupled thereto, the set-top box sending said first message to said server in response to authentication of said smart card and said service provider identification data.

9. (Currently Amended) The method of Claim 8 wherein said ~~second identification~~ digital certificate data ~~further~~ comprises data associated with ~~said~~ a certificate authority and data associated with the validity of said digital certificate.

10. (Previously Presented) A method for managing access to an electronic device, said method comprising:

(a) sending first identification data associated with a first electronic device to a second electronic device;

(b) receiving, in said first device, from said second device a digital certificate encrypted using a first private key of said second device, said digital certificate having second identification data associated with said second device and a second public key of said second device;

(c) encrypting said first identification data in said second device using a second private key associated with said second device to generate first encrypted identification data;

(d) receiving, in said first device, from said second device said first encrypted identification data;

(e) decrypting in said first device, using a first public key to obtain said second public key, said encrypted digital certificate received from said second device, said first public key being stored in said first device;

(f) decrypting said first encrypted identification data using said second public key to generate a first decrypted identification data;

(g) authenticating said second device by comparing said first decrypted identification data to said first identification data;

(h) sending to said second device second encrypted identification data, said second encrypted identification data being encrypted in said first device using said second public key of said second device; and

(i) establishing a communication channel between said first and said second devices.

Claims 11-20. (Cancelled)

21. (Currently Amended) A method for managing access between a plurality of electronic devices, comprising:

sending first message data from a first electronic device to a second electronic device;

receiving, in said first device, from said second device, second data being indicative of a digital certificate encrypted using a first private key of said second device;

receiving, in said first device, from said second device, said first message data being encrypted using a second private key of said second device;

authenticating said second device in response to said digital certificate and said first encrypted message;

~~establishing a communication channel between said first and said second devices in response to the authentication of said second device;~~

encrypting said first message using a public key related to the second private key of said second device to generate a second encrypted message; ~~and~~

sending data indicative of said second encrypted message to said second device; and

establishing a communication channel between said first and said second devices in response to the authentication of said second device.

22. (Currently Amended) A method for managing access between a plurality of electronic devices, comprising:

sending first message data from a first electronic device to a second electronic device, the first message data comprising first identification data associated with said first device and a date and time stamp;

receiving, in said first device, from said second device digital certificate data encrypted using a first private key of said second device, said digital certificate data comprising second identification data associated with said second device and a second public key of said second device;

receiving, in said first device, from said second device said first message data encrypted using a second private key of said second device;

authenticating said second device in response to said digital certificate data and said encrypted first message data;

~~establishing a communication channel between said first and said second devices in response to the authentication of said second device;~~

encrypting said first message data using a public key related to the second private key of said second device to generate a second encrypted message data; [[and,]]

sending said second encrypted message data to said second device; and

establishing a communication channel between said first and said second devices in response to the authentication of said second device;

wherein, said authenticating comprises: decrypting said digital certificate in said first device using a first public key stored in said first device; decrypting said first encrypted message using said public key used to generate said second encrypted message to generate a first decrypted message; and comparing said first decrypted message to said first message.